mathworld

INDEX
Algebra
Applied Mathematics
Calculus and Analysis
Discrete Mathematics
Foundations of Mathematics
Geometry
History and Terminology
Number Theory
Probability and Statistics
Recreational Mathematics
Topology
Alphabetical Index

ABOUT THIS SITE
About *MathWorld*
About the Author
Terms of Use

DESTINATIONS
What's New
Headline News (RSS)
Random Entry
Animations
Live 3D Graphics

CONTACT
Email Comments
Contribute!
Sign the Guestbook

MATHWORLD - IN PRINT
Order book from Amazon

Algebra » **Cyclotomy** »
Discrete Mathematics » **Recurrence Equations** »
Recreational Mathematics » **Interactive Entries** » **Animated GIFs** »

Cyclotomic Polynomial

A polynomial given by

$$\Phi_n(x) = \prod_{k=1}^{n'} (x - \zeta_k),$$

where ζ_k are the roots of unity in $\mathbb{C}$ given by

$$\zeta_k \equiv e^{2\pi i k/n}$$

and k runs over integers relatively prime to n. The prime may be dropped if the instead taken over primitive roots of unity, so that

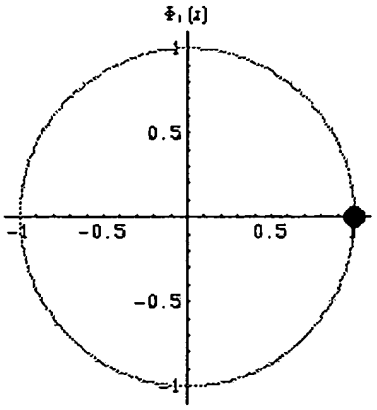
$$\Phi_n(x) = \prod_{\substack{k=1 \\ \text{primitive } \zeta_k}}^{n} (x - \zeta_k).$$

The notation $F_n(x)$ is also frequently encountered. Dickson *et al.* (1923) and I (1975) give extensive bibliographies for cyclotomic polynomials.

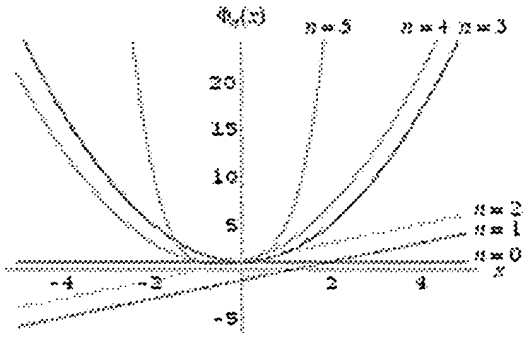
The cyclotomic polynomial for $n > 1$ can also be defined as

$$\Phi_n(x) = \prod_{d|n} (1 - x^{n/d})^{\mu(d)}$$

where $\mu(d)$ is the Möbius function and the product is taken over the divisors d 1991, p. 225).



$\Phi_n(x)$ is an integer polynomial and an irreducible polynomial with polynomial $\phi(n)$, where $\phi(n)$ is the totient function. Cyclotomic polynomials are returned *Mathematica* command `Cyclotomic[n, x]`. The roots of cyclotomic polynomials l unit circle in the complex plane, as illustrated above for the first few cyclotomic polynomials.



The first few cyclotomic polynomials are

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = x^2 - x + 1$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_8(x) = x^4 + 1$$

$$\Phi_9(x) = x^6 + x^3 + 1$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

If p is an odd prime, then

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

$$\Phi_{2p}(x) = \frac{x^{2p} - 1}{x^p - 1}\frac{x - 1}{x^2 - 1} = x^{p-1} - x^{p-2} + \ldots - x + 1$$

$$\Phi_{4p}(x) = \frac{x^{4p} - 1}{x^{2p} - 1}\frac{x^2 - 1}{x^4 - 1} = x^{2p-2} - x^{2p-4} + \ldots - x^2 + 1$$

(Riesel 1994, p. 306). Similarly, for p again an odd prime,

$$x^p - 1 = \Phi_1(x)\Phi_p(x)$$

$$x^{2p} - 1 = \Phi_1(x)\Phi_2(x)\Phi_p(x)\Phi_{2p}(x)$$

$$x^{4p} - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_p(x)\Phi_{2p}(x)\Phi_{4p}(x).$$

For the first few remaining values of n,

$$x - 1 = \Phi_1(x)$$

$$x^2 - 1 = \Phi_1(x)\Phi_2(x)$$

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)$$

$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$$

$$x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x)$$

$$x^{15} - 1 = \Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)$$

$$x^{16} - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)\Phi_{16}(x)$$

$$x^{18} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)\Phi_9(x)\Phi_{18}(x)$$

(Riesel 1994, p. 307).

For p a prime relatively prime to n,

$$F_{np}(x) = \frac{F_n(x^p)}{F_n(x)},$$

but if $p|n$,

$$F_{np}(x) = F_n(x^p)$$

(Nagell 1951, p. 160).

An explicit equation for $\Phi_n(x)$ for squarefree *n* is given by

$$\Phi_n(x) = \sum_{j=0}^{\phi(n)} a_{nj} x^{\phi(n)-j},$$

where a_{nj} is calculated using the recurrence relation

$$a_{nj} = -\frac{\mu(n)}{j} \sum_{m=0}^{j-1} a_{nm} \mu(\mathrm{GCD}(n, j-m)) \phi(\mathrm{GCD}(n, j-m)),$$

with $a_{n0} = 1$, where $\mu(n)$ is the Möbius function and $\mathrm{GCD}(m, n)$ is the gre common denominator of *m* and *n*.

The polynomial $x^n - 1$ can be factored as

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where $\Phi_d(x)$ is a cyclotomic polynomial. Furthermore,

$$x^n + 1 = \frac{x^{2n} - 1}{x^n - 1} = \frac{\prod_{d|2n} \Phi_d(x)}{\prod_{d|n} \Phi_d(x)}.$$

The coefficients of the inverse of the cyclotomic polynomial

$$\frac{1}{1 + x + x^2} = 1 - x + x^3 - x^4 + x^6 - x^7 + x^9 - x^{10} + \ldots$$

$$= \sum_{n=0}^{\infty} c_n x^n$$

can also be computed from

$$\begin{aligned} c_n &= 1 - 2\left\lfloor \tfrac{1}{3}(n+2) \right\rfloor + \left\lfloor \tfrac{1}{3}(n+1) \right\rfloor + \left\lfloor \tfrac{1}{3} n \right\rfloor \\ &= 1 - 3\left\lfloor \tfrac{1}{3}(n+2) \right\rfloor + \lfloor n \rfloor \\ &= \frac{2}{\sqrt{3}} \sin\left[\tfrac{2}{3}\pi(n+1)\right], \end{aligned}$$

where $\lfloor x \rfloor$ is the floor function.

For p prime,

$$\Phi_p(x) = \sum_{k=0}^{p-1} x^k,$$

i.e., the coefficients are all 1. The first cyclotomic polynomial to have a coefficie than ± 1 and 0 is $\Phi_{105}(x)$, which has coefficients of -2 for x^7 and x^{41}. This i because 105 is the first number to have three distinct odd prime factors, i.e., $105 = 3 \cdot 5 \cdot 7$ (McClellan and Rader 1979, Schroeder 1997). The smallest val which $\Phi_n(x)$ has one or more coefficients ± 1, ± 2, ± 3, ... are 0, 105, 385, 1 2805, 3135, 6545, 6545, 10465, 10465, 10465, 10465, 10465, 11305, ... (Slo A013594).

It appears to be true that, for $m, n > 1$, if $\Phi_m(x) + \Phi_n(x)$ factors, then the contain a cyclotomic polynomial. For example,

$$\Phi_7(x) + \Phi_{22}(x) = (x^2 + 1)(x^8 - x^7 + 2x^4 + 2) = \Phi_4(x)(x^8 - x^7 + 2x^4$$

This observation has been checked up to $m, n = 150$ (C. Nicol). If m and n ar then $C_m + C_n$ is irreducible.

Migotti (1883) showed that coefficients of $\Phi_{pq}(x)$ for p and q distinct primes c 0, ± 1. Lam and Leung (1996) considered

$$\Phi_{pq}(x) = \sum_{k=0}^{pq-1} a_k x^k$$

for p, q prime. Write the totient function as

$$\phi(pq) = (p-1)(q-1) = rp + sq$$

and let

$$0 \le k \le (p-1)(q-1),$$

then

1. $a_k = 1$ iff $k = ip + jq$ for some $i \in [0, r]$ and $j \in [0, s]$,
2. $a_k = -1$ iff $k + pq = ip + jq$ for $i \in [r+1, q-1]$ and $j \in [s+$
3. otherwise $a_k = 0$.

The number of terms having $a_k = 1$ is $(r+1)(s+1)$, and the number of te $a_k = -1$ is $(p-s-1)(q-r-1)$. Furthermore, assume $q > p$, then the m

coefficient of Φ_{pq} is $(-1)^r$.

Resultants of cyclotomic polynomials have been computed by Lehmer (1930), D (1940), and Apostol (1970). It is known that $\rho(\Phi_k(x), \Phi_n(x)) = 1$ if (m, n) m and n are relatively prime (Apostol 1975). Apostol (1975) showed that for po integers m and n and arbitrary nonzero complex numbers a and b,

$$\rho(\Phi_m(ax), \Phi_n(bx)) = b^{\phi(m)\phi(n)} \prod_{d|n} \left[\Phi_{m/\delta}\left(\frac{a^d}{b^d}\right)\right]^{\mu(n/d)\phi(m)/\phi(m/\delta)}$$

where $\delta = \mathrm{GCD}(m, d)$ is the greatest common divisor of m and d, $\phi(n)$ is tl function, $\mu(n)$ is the Möbius function, and the product is over the divisors of n are distinct primes p and q, then (44) simplifies to

$$\rho(\Phi_q(ax), \Phi_p(bx)) = \begin{cases} \frac{a^{pq}-b^{pq}}{a^p-b^p}\frac{a-b}{a^q-b^q} & \text{for } a \neq b \\ a^{(p-1)(q-1)} & \text{for } a = b. \end{cases}$$

The following table gives the resultants $\rho(\Phi_k(x), \Phi_n(x))$ (Sloane's A054372).

$k\backslash n$	1	2	3	4	5	6	7
1	0						
2	2	0					
3	3	1	0				
4	2	2	1	0			
5	5	1	1	1	0		
6	1	3	4	1	1	0	
7	7	1	1	1	1	1	0

The numbers of 1s in successive rows of this table are given by 0, 0, 1, 1, 3, 3, 9, ... (Sloane's A075795).

The cyclotomic polynomial $\Phi_6(x)$ has the particularly nice Maclaurin series

$$\frac{1}{\Phi_6(x)} = 1 + x - x^3 - x^4 + x^6 + x^7 - x^9 - x^{10} + \ldots,$$

whose coefficients 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, ... (Sloane's A010892) are giv solving the recurrence equation

$$a(n) = a(n-1) - a(n-2)$$

with $a(0) = a(1) = 1$ (Wolfram 2002, p. 128), giving the explicit form

$$a(n) = \frac{2}{3}\sqrt{3}\sin[\tfrac{1}{3}(n+1)\pi].$$

Interestingly, any sequence $b(n)$ satisfying the linear recurrence equation

$$b(n) = b(n-1) - b(n-2)$$

can be written as

$$b(n) = b(0)a(n) + [b(1) - b(0)]a(n-1).$$

SEE ALSO: Aurifeuillean Factorization, Gauss's Cyclotomic Formula, Lucas's Theor Inversion Formula, Primitive Root of Unity, Root of Unity

RELATED WOLFRAM SITES: http://functions.wolfram.com/Polynomials/Cyclot

PAGES LINKING HERE: search

REFERENCES:

Apostol, T. M. "Resultants of Cyclotomic Polynomials." *Proc. Amer. Math. Soc.* **24**, 457-462, 19

Apostol, T. M. "The Resultant of the Cyclotomic Polynomials $F_m(ax)$ and $F_n(bx)$." *Math.* 1-6, 1975.

Beiter, M. "The Midterm Coefficient of the Cyclotomic Polynomial $F_{pq}(x)$." *Amer. Math. Monti* 770, 1964.

Beiter, M. "Magnitude of the Coefficients of the Cyclotomic Polynomial F_{pq}." *Amer. Math. Mon* 372, 1968.

Bloom, D. M. "On the Coefficients of the Cyclotomic Polynomials." *Amer. Math. Monthly* **75**, 37

Brent, R. P. "On Computing Factors of Cyclotomic Polynomials." *Math. Comput.* **61**, 131-149, 1

Carlitz, L. "The Number of Terms in the Cyclotomic Polynomial $F_{pq}(x)$." *Amer. Math. Monthl* 981, 1966.

Conway, J. H. and Guy, R. K. *The Book of Numbers.* New York: Springer-Verlag, 1996.

de Bruijn, N. G. "On the Factorization of Cyclic Groups." *Indag. Math.* **15**, 370-377, 1953.

Dickson, L. E.; Mitchell, H. H.; Vandiver, H. S.; and Wahlin, G. E. *Algebraic Numbers.* Bull Nat. Vol. 5, Part 3, No. 28. Washington, DC: National Acad. Sci., 1923.

Diederichsen, F.-E. "Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetisch Äquivalenz." *Abh. Math. Sem. Hanisches Univ.* **13**, 357-412, 1940.

Lam, T. Y. and Leung, K. H. "On the Cyclotomic Polynomial $\Phi_{pq}(X)$." *Amer. Math. Monthly* 1

1996.

Lehmer, E. "On the Magnitude of the Coefficients of the Cyclotomic Polynomial." *Bull. Amer. Ma* 389-392, 1936.

Lehmer, E. "On the Magnitude of Coefficients of the Cyclotomic Polynomials." *Bull. Amer. Math.* 389-392, 1936.

McClellan, J. H. and Rader, C. *Number Theory in Digital Signal Processing.* Englewood Cliffs, NJ: Hall, 1979.

Migotti, A. "Zur Theorie der Kreisteilungsgleichung." *Sitzber. Math.-Naturwiss. Classe der Kaiser Wiss., Wien* **87**, 7-14, 1883.

Nagell, T. "The Cyclotomic Polynomials" and "The Prime Divisors of the Cyclotomic Polynomial." in *Introduction to Number Theory.* New York: Wiley, pp. 158-160 and 164-168, 1951.

Riesel, H. "The Cyclotomic Polynomials" in Appendix 6. *Prime Numbers and Computer Methods Factorization, 2nd ed.* Boston, MA: Birkhäuser, pp. 305-308, 1994.

Schroeder, M. R. *Number Theory in Science and Communication, with Applications in Cryptogra Digital Information, Computing, and Self-Similarity, 3rd ed.* New York: Springer-Verlag, p. 245,

Séroul, R. "Cyclotomic Polynomials." §10.8 in *Programming for Mathematicians.* Berlin: Springe pp. 265-269, 2000.

Sloane, N. J. A. Sequences A013594, A010892, A054372, and A075795 in "The On-Line Encycl Integer Sequences." http://www.research.att.com/~njas/sequences/.

Trott, M. "*The Mathematica Guidebooks* Additional Material: Graphics of the Argument of Cyclot Polynomials." http://www.mathematicaguidebooks.org/additions.shtml#N_2_03.

Vardi, I. *Computational Recreations in Mathematica.* Redwood City, CA: Addison-Wesley, pp. 8 1991.

Wolfram, S. *A New Kind of Science.* Champaign, IL: Wolfram Media, 2002.

CITE THIS AS:
Eric W. Weisstein. "Cyclotomic Polynomial." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/CyclotomicPolynomial.html